UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

PROXENSE, LLC, *Plaintiffs*, v. SAMSUNG ELECTRONICS, CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC, *Defendants*.	Civil Action No. 6.21-CV-00210 **JURY TRIAL REQUESTED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Proxense, LLC ("Proxense" or "Plaintiff") hereby sets forth its Complaint for patent infringement against Defendants Samsung Electronics Co., Ltd. ("SEC") and Samsung Electronics America, Inc. ("SEA") (collectively, "Samsung" or "Defendants"), and states as follows:

NATURE OF THE CASE

1. This action is for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, et seq. As further stated herein, Proxense alleges that Samsung infringes one or more claims of patents owned by Proxense. Accordingly, Proxense seeks monetary damages and injunctive relief in this action.

THE PARTIES

2. Plaintiff Proxense, LLC is a Delaware company with its principal place of business at 689 NW Stonepine Drive, Bend, Oregon 97703.

3. Upon information and belief, SEC is a corporation organized under the laws of the Republic of Korea, having a place of business at 129, Samsung-Ro, Yeongtong-Gu, Gyeonggi,

16677, Republic of Korea. SEC may be served with process pursuant to Federal Rule of Civil Procedure 4(f)(1).

4. Upon information and belief, SEA is a corporation organized under the laws of New York, having a principal place of business at 85 Challenger Rd., Ridgefield Park, NJ 97660. SEA maintains a place of business in this District at 12100 Samsung Blvd., Austin, TX 78754. SEA may be served with process through its registered agent, CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201.

5. SEC designs, manufactures, and provides to the United States and other markets a wide variety of hardware and software products and services, including consumer electronics, mobile phones, handheld devices, tablets, laptops and other personal computers, storage devices, televisions, and electronic devices.

6. Upon information and belief, SEA is a wholly-owned subsidiary of SEC and is responsible for domestic distribution of Samsung's consumer products, including the products accused of infringement herein.

JURISDICTION AND VENUE

7. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

8. This Court has personal jurisdiction over Samsung because it has conducted and continues to regularly conduct business within the State of Texas and this District. Samsung has purposefully and voluntarily availed itself of the privileges of conducting business in the United States, the State of Texas, and this District by continuously and systematically placing goods into

the stream of commerce through an established distribution channel with the expectation that they will be purchased by consumers in this District. Samsung directly and/or through intermediaries (including distributors, sales agents, and others), ships, distributes, sells, offers to sell, imports, advertises, makes, and/or uses its products (including but not limited to the products accused of infringement herein) in the United States, the State of Texas, and this District.

9. SEA is registered to do business in Texas and maintains an agent for service of process in Texas. SEA maintains places of business within the Western District of Texas, including at 12100 Samsung Blvd., Austin, TX 78754.

10. Upon information and belief, Samsung has authorized retailers that offer and sell products on its behalf in this District, including products accused of infringement herein. Upon information and belief, these include Walmart, *e.g.*, Supercenter #939, 4230 Franklin Ave., Waco, TX 76710; Target, *e.g.*, at 5401 Bosque Blvd., Waco, TX 76710; Best Buy, *e.g.*, at 4627 S. Jack Kultgen Expy., Waco, TX 76706; T-Mobile Store, *e.g.,* at 1107 N Valley Mills Dr., Bldg 1, Waco, TX 76710; and Verizon, *e.g.*, at 1820 S Valley Mills Dr., Waco, TX 76711, among many others.

11. Proxense's causes of action arise directly from Samsung's business contacts and other activities in the State of Texas and this District.

12. Samsung has derived substantial revenues from its infringing acts within the State of Texas and this District.

13. Venue is proper in this District as to SEC pursuant to 28 U.S.C. § 1391(c)(3) because it is not a resident of the United States and may therefore be sued in any judicial district.

14. Venue is proper in this District as to SEA pursuant to 28 U.S.C. § 1400(b) because SEA has committed acts of infringement in this District and has regular and established places of business in this District.

15. Joinder of SEC and SEA is proper because they are related entities that are either jointly and severally liable for infringement, or that make, use, sell, offer to sell, and/or import the same or similar products accused of infringement herein. Further, upon information and belief, SEC and SEA use the same underlying hardware and/or software in their infringing products and therefore the factual question of infringement will substantially overlap between SEC and SEA. Proxense anticipates there will be substantial overlap with respect to discovery.

16. Samsung has committed acts of infringement in this District and does business in this District, including making sales and/or providing service and support for customers and/or end-users in this District. Samsung purposefully and voluntarily sold one or more infringing products with the expectation they would be purchased in this District. These infringing products have been and continue to be purchased in this District. Thus, Samsung has committed acts of infringement within the United States, the State of Texas, and this District.

PATENTS-IN-SUIT

17. On January 8, 2013, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,352,730 (the "730 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 730 Patent is attached hereto as **Exhibit 1**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=08352730.

18. On March 26, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,298,905 (the "905 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 905 Patent is attached hereto as **Exhibit 2**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09298905.

19. On June 30, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,698,989 (the "989 Patent") entitled "Biometric personal data key (PDK)

authentication." A true and correct copy of the 989 Patent is attached hereto as **Exhibit 3**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=10698989.

20. On June 2, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,049,188 (the "188 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder circuit and Methods of Use." A true and correct copy of the 188 Patent is attached hereto as **Exhibit 4**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09049188.

21. On January 12, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,235,700 (the "700 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder circuit and Methods of Use." A true and correct copy of the 700 Patent is attached hereto as **Exhibit 5**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09235700.

22. Proxense is the sole and exclusive owner of all right, title and interest to and in, or is the exclusive licensee with the right to sue for, the 730, 905, 989, 188, and 700 Patents (together, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Proxense also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

23. The technologies of the Patents-in-Suit were invented by John Giobbi and David L. Brown. The 730 and 905 Patents generally cover systems and methods for an integrated device that persistently stores biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (*e.g.*, a finger-print) can be compared against the stored biometric data. Once the user has been biometrically verified by the integrated device, a code can be wirelessly

transmitted for authentication. The 989 Patent generally covers systems and methods of verifying a user during authentication of an integrated device.

24. The 188 and 700 Patents generally covers a hybrid device including a personal digital key ("PDK") and receiver-decoder circuit ("RDC"), wherein the PDK and RDC are coupled for communication with each other. The 188 and 700 Patents also includes a number of system configurations for use of the hybrid device including: use of the hybrid device in a cell phone; simultaneous use of the PDK and the RDC functionality of hybrid device; use of multiple links of hybrid device to generate an authorization signal, use of multiple PDK links to the hybrid device to generate an authorization signal; and use of the hybrid device for authorization inheritance.

FACTUAL ALLEGATIONS

I. TECHNOLOGY BACKGROUND

25. Global contactless transaction values were estimated at $2 trillion in 2020. By 2024, they may reach $6 trillion according to forecasts. Mobile payments, or transactions initiated on mobile devices such as cell phones or tablet computers, have become increasingly popular as applications like Samsung Pay, launched in 2015, come bundled with Samsung's popular devices, like the Galaxy-branded line of phones. According to Samsung, "consumers have relied on Samsung Pay to make billions of transactions." Mobile payments can include payments for goods and services purchased over the internet (*e.g.,* through merchant websites or applications), or payments at a point of sale, which are payments initiated from a mobile device at a physical location.

26. Near Field Communication ("NFC") is a form of contactless communication between devices that allows two NFC-equipped devices placed within a few centimeters of each other to exchange data. NFC technology provides power consumption and ease-of-use advantages

as compared to other methods of close-proximity wireless communication (*e.g.*, Bluetooth). NFC can be used to facilitate mobile payments when an NFC-equipped device (such as a smartphone or electronic wearable like a watch) is placed near a contactless merchant terminal, allowing the devices to exchange payment data.

27. Contactless merchant terminal adoption in the U.S. has been expedited by card issuer security requirements. Card issuers in the United States set an October 2015 deadline for merchants to upgrade payment terminals capable of accepting credit cards with embedded chips for security, and many of these upgraded terminals have NFC capability built in. In December 2015, approximately 2.36 million contactless terminals were in service in the United States. As a result of the COVID-19 pandemic, there has been a sharp rise in adoption of contactless payment all over the globe.

28. Magnetic Secure Transmission ("MST") is a technology that emits a magnetic signal to mimic the magnetic strip on a traditional payment card. MST technology can be used to facilitate mobile payments when an MST-equipped device is placed near a merchant terminal, allowing the devices to exchange data. MST does not generally require merchants to upgrade payment terminal software or hardware. The technology was developed to facilitate contactless payments on point-of-sale terminals that can accept only conventional magnetic stripe cards. LoopPay, a contactless payments company that utilized MST (and was acquired by Samsung), claimed a 90% merchant acceptance rate.

II. PROXENSE AND ITS INNOVATIVE TECHNOLOGIES

29. Proxense was founded in 2001 as a limited venture. The company was formally incorporated in 2005 as an LLC. From approximately 2004-2012, Proxense developed, *inter alia*, mobile payment technologies and commercial products, employing over thirty engineers, and

investing many millions of dollars in product development and other research and development efforts. Foundational capabilities of Proxense's technologies included a secure element, biometrics captured and stored thereon, retrieval of biometrics and token passing to a trusted third party, and completion of a mobile payment transaction.

30. Proxense also developed sophisticated, proprietary, proximity-based detection, authentication, and automation technology, built on the concept of utilizing small electronic sensors, or receiver-decoder circuits ("RDCs"), capable of wirelessly detecting, authenticating, and communicating with personal digital keys ("PDKs"). Proxense's technology enabled PDKs to run for as long as two years on tiny batteries. "ProxPay" technology also included biometrically-based user and device authentication options, the ability to conduct biometric-verified transactions without sending or exposing the underlying biometric data or storing it anywhere except the PDK, and the incorporation of a registration for maintaining or verifying the PDK. Significant financial and engineering resources were deployed to make this possible. The resulting developments became primary differentiators of Proxense's product line, and significant elements on which its business was built.

31. John Giobbi is the founder and CEO of Proxense. He is an experienced product designer and prolific inventor (a named inventor on approximately 200 patents, including three of the asserted patents), with over 35 years of experience as an entrepreneur and product development executive. For example, Mr. Giobbi was a Senior Vice President at WMS Gaming, and managed over 200 staff; in his six-year tenure at that company, its market capitalization soared from approximately $80 million to about $1 billion. Mr. Giobbi was also the founder and President of Prelude Technology Corp. and InPen.

32. The innovative, visionary nature of Proxense's technology was recognized in the media, beginning in mid-2008, when, The Bulletin featured a story on Proxense's mobile payment technology, titled "A pint-sized virtual wallet." Andrew Moore, The Bulletin (May 7, 2008), **Exhibit 6**. The story describes a future that greatly resembles the present-day, including a "wireless wallet" and "fingerprint" verification, including the use of such technology to pay for goods using such wireless methods protected by biometric measures like a fingerprint. In 2009, Trend Hunter ran a similar story titled "Virtual Biometric Wallets," featuring Proxense and Mr. Giobbi. Michael Plishka, Trend Hunter (January 4, 2009), **Exhibit 7**.

33. Another 2009 article, ran in DARKReading, a publication in InformationWeek's IT Network, also featured the company and Mr. Giobbi in an article titled "Startup May Just Digitize Your Wallet." George V. Hulme, DARKReading (February 8, 2009), **Exhibit 8**. The DARKReading article described that Proxense was "in the process of bringing to market a proximity-based communications device that aims to provide a way to securely share information and conduct payments." Proxense's Personal Digital Keys (PDKs) were described as "carried by users, perhaps even within a cell phone, and can security hold data and manage authentication." Mr. Giobbi explained that "the data within the PDK also can be protected by additional layers of authentication, such as biometric…"

34. It would be years until products like Apple Pay (2014) and Samsung Pay (2015) were launched and became mainstream; Apple's TouchID, which involves fingerprint recognition technology, and Samsung's fingerprint scanner on its own phones, were introduced in 2013 and 2014, respectively. Accordingly, Proxense's technology was years ahead of the industry.

35. After the launch of services like Samsung Pay, and its inextricable link to the some of the most popular smartphone hardware devices in the United States, and the world, Proxense

would find itself unable to compete with companies like Samsung, even though Proxense invented the technology utilized in these solutions.

36. Today, Proxense holds at least 65 patents on related technology, including digital content distribution, digital rights management, personal authentication, biometric data management and mobile payments. Proxense continues to prosecute new patents on its proprietary technology.

III. INFRINGEMENT ALLEGATIONS

1. Proxense's Interactions with Samsung

37. In or around April 2017, Proxense was introduced to Samsung. Since at least that time, Samsung has had constructive notice of the Patents-in-Suit and the scope of their claims as of at least their dates of issue. Proxense has given Samsung actual notice of the Patents-in-Suit, and also placed Samsung on notice of the Patents-in-Suit as of the date of public filing of this Complaint.

38. Samsung has also had knowledge of the infringing nature of its activities, or at least a willful blindness regarding the infringing nature of its activities, since at least Proxense's making Samsung aware of the Patents-in-Suit, if not as of the public filing of this Complaint.

39. Despite Samsung's knowledge of the Patents-in-Suit, and its constructive knowledge of its infringing actions, Samsung continued to infringe the claims of the Patents-in-Suit. Samsung's infringement has been and continues to be willful since at least the date of the public filing of this Complaint.

2. The Accused Products

40. Samsung has manufactured, used, marketed, distributed, sold, offered for sale, and exported from and imported into the United States devices and software that directly and/or

indirectly infringe (literally or via the doctrine of equivalents) the Patents-in-Suit. Samsung has distributed variants of Samsung Pay that have included functionality to verify a user during authentication of a smartphone. Samsung Pay is operable on a range of Samsung devices, including at least all smartphones from the Galaxy S6 and above, including but not limited to, at least the Samsung devices set forth in **Appendix A**, including Galaxy S21, S20+, S21 Ultra, Galaxy S20, S20+, S20 Ultra 5G, Galaxy Fold, Galaxy Z-Flip, ZFlip 5G, Galaxy Note 20, Note 20 Ultra, Note10, Note10+, Note10+ 5G, Note5, Galaxy S10e, S10, S10+, Galaxy Note9, Galaxy S9, S9+, Galaxy Note8, Galaxy Note5, Galaxy S8, S8+, Galaxy S7, S7 edge, Galaxy S6, S6 edge, S6 edge+, S6 Active, Galaxy A90, Galaxy A80, Galaxy A70, A71, A71 5G, Galaxy A50, A51, Galaxy A40, Galaxy A30, A31, Galaxy A20e, Galaxy A8, Galaxy A7, Galaxy A5, Galaxy J7, Galaxy J5 Pro, Galaxy Watch S3, Galaxy Watch S2 Sport, Galaxy Watch S2 Classic, Gear S3 Frontier, Gear S3 Classic, Galaxy Watch Active 2, Galaxy Watch Active, Galaxy Watch, Gear Sport, Gear S3, and Gear S2, and all Samsung devices released since September 2015. The current and previous versions of Samsung Pay and devices with Samsung Pay, alone and together, are non-limiting instances of the Accused Products. The Accused Products practice the claims of the Patents-in-Suit to improve the shopping experience of their users, and to improve Samsung's position in the market.

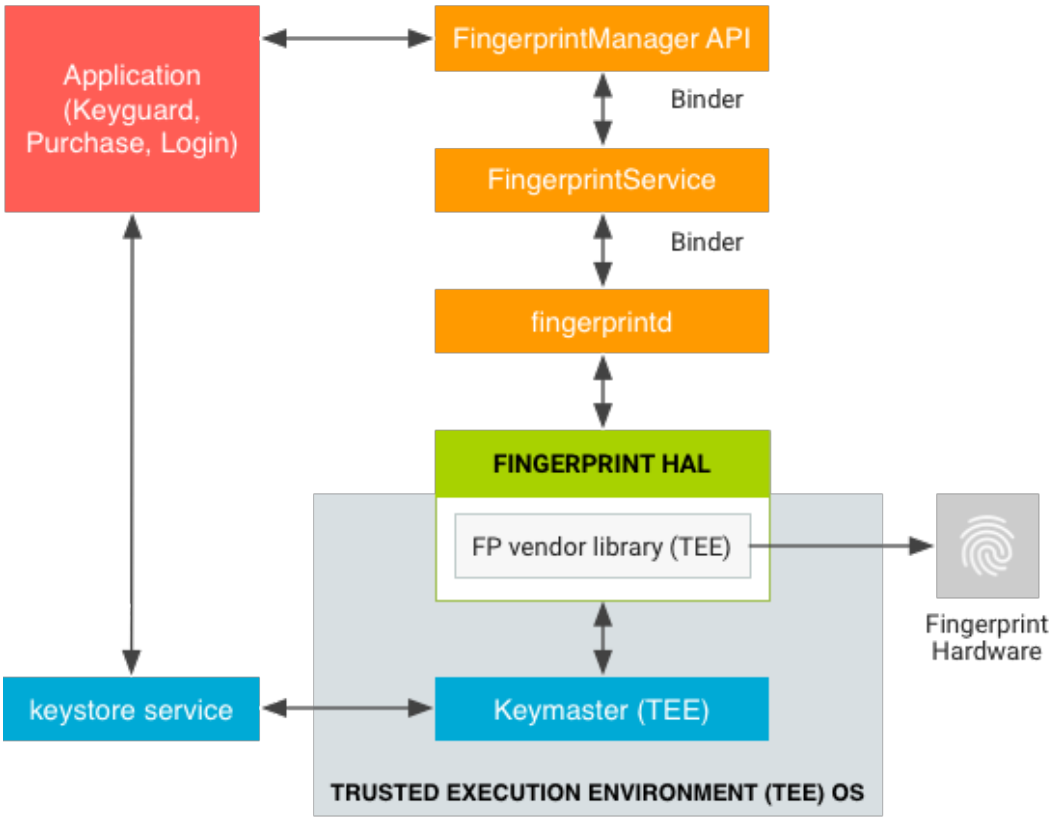
3. Samsung's Infringement of the Patents-in-Suit

41. Samsung Pay is described by Samsung as "an easy way to make purchases on your phone or watch." "It turns your device into a digital wallet that carries credit, debit, or gift cards." "And don't worry, you can use biometric security, so no one can access your financial data." Samsung advertises that "Samsung Pay is only available on select phone and watch models" and

that Samsung Pay may be used on a smart watch with a non-Samsung phone running Android 6.0 or later. **Exhibit 9 (Set up Samsung Pay on your phone, Samsung Support)**.

42. On information and belief, Samsung phones utilize Android's Fingerprint Hardware Interface Definition Language ("HIDL") to connect to its vendor-specific library and fingerprint hardware (e.g., a fingerprint sensor); to implement the Fingerprint HIDL, Samsung implements IBiometricsFingerprint.hal (the "Fingerprint HAL") in its vendor-specific library. Biometric data is protected because fingerprint templates must be signed with a private, device-specific key under the Fingerprint HIDL implemented by Samsung.

43. Fingerprint HAL interacts with Keystore Application Programming Interface ("API") and Keymaster components which provide hardware-backed cryptography for secure key storage in a secure environment, such as the Trusted Execution Environment ("TEE"). A high-level data flow for fingerprint authentication is produced below:

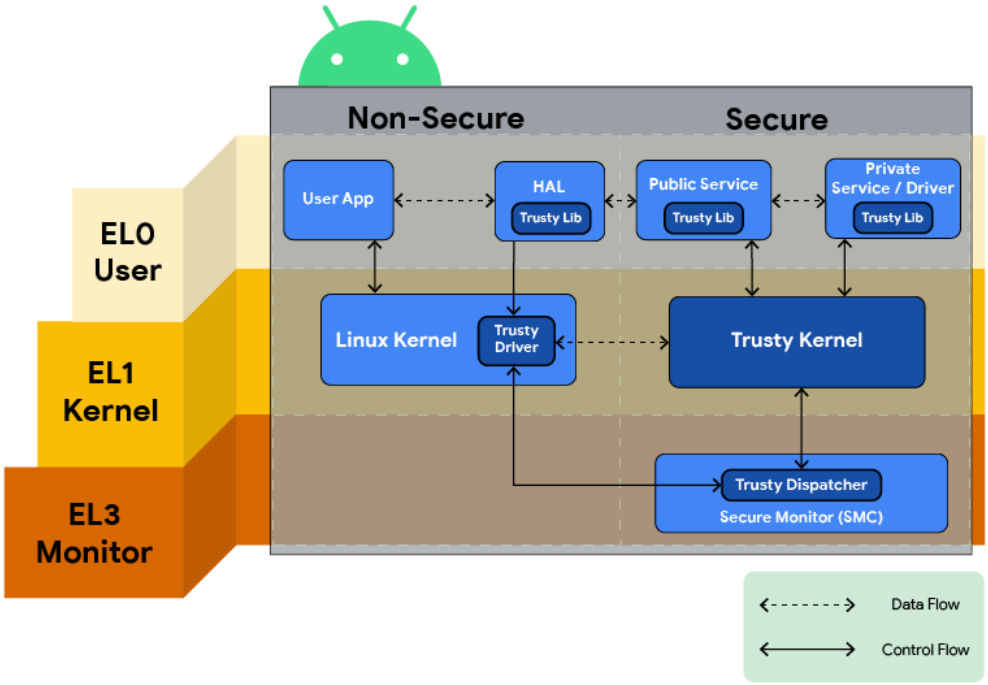


44. Keymaster functions include private key operations (*e.g.*, KeyPurpose:DECYPT and KeyPurpose::SIGN), e.g. a secret decryption value.

45. The Fingerprint HAL guidelines are described in the Android documentation as being designed to ensure that fingerprint data is not leaked and is removed when a user is removed from a device: Raw fingerprint data or derivatives (for example, templates) must never be accessible from outside the sensor driver or TEE. If the hardware supports a TEE, hardware access must be limited to the TEE and protected by an SELinux policy. The Serial Peripheral Interface (SPI) channel must be accessible only to the TEE and there must be an explicit SELinux policy on all device files. Fingerprint acquisition, enrollment, and recognition must occur inside the TEE.

46. "Trusty" is a secure Operating System ("OS") that provides a Trusted Execution Environment for Android, the operating system run on Samsung's smartphone devices. On information and belief, on Samsung's smartphone products, the Trusty OS runs on the same processor as the Android OS, and the two OS's run parallel to each other. Trusty has access to the full power of a device's main processor and memory but is completely isolated from the rest of the system by both hardware and software. Trusty's isolation protects it from malicious apps installed by the user and potential vulnerabilities that may be discovered in Android.

47. On ARM systems, like Samsung's devices, Trusty uses ARM's Trustzone™ to virtualize the main processor and create a secure TEE. An overview diagram of Trusty is reproduced below:



48. Uses for a TEE like Trusty include mobile payments, secure banking, multi-factor authentication, device reset protection, replay-protected persistent storage, and secure PIN and fingerprint processing.

49. Samsung describes that "[w]ith Samsung Pay, each transaction is covered by your bank's fraud protection and authenticated by your fingerprint, PIN or iris scan." "Plus, Samsung Knox and tokenization add extra layers of security." See **Exhibit 10 (Samsung Pay Website)**.

50. According to Samsung, Samsung Pay uses three levels of security to enable secure payments: fingerprint or iris-scanning authentication, tokenization and Samsung Knox, Samsung's defense-grade mobile security platform.

51. Samsung Knox "builds upon the Android Keystore by providing a tamper-proof, detection-based lock-down of cryptographic keys." On Samsung devices utilizing Knox, "the authentication software doesn't share or distribute the biometric measurements of any user." **Exhibit 11** (Knox Platform for Enterprise, Version 1.3.1 (2020)), page 41. "The measurements are stored in a format that can't be used to reproduce the original biometric, and can only be

accessed and decoded within the specific part of the TrustZone that has access to the biometric hardware." *Id*.

52. Visa has described Samsung Pay as "a simple way for customers to pay that meets all 2015 EMV security standards." *See* **Exhibit 12 (Visa and Samsung Pay)** . EMV, which originally stood for "Europay, Mastercard, and Visa", the three companies which created the standard, is a payment method based upon a technical standard for smart payment cards and for payment terminals and automated teller machines which can accept them.

53. EMVCo, LLC ("EMVCo") facilitates worldwide interoperability and acceptance of secure payment transactions. EMVCo is supported by dozens of banks, merchants, processors, vendors and other industry stakeholders, including Samsung. EMVCo manages and evolves the EMV Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Samsung has received approval for the accused products as EMV Contactless Level 1 Mobile Products, *e.g.*, recently for the Samsung Galaxy S21 5G, Product Name SM-G991U. The publicly available approval letters, attached hereto as **Exhibit 13**, describe that EMVCo received a request for approval and found reasonable evidence that the submitted samples sufficiently conform to the EMV Contactless Interface Specification and other EMVCo requirements. Notably, EMV specifications were first published in 2007, years after the priority dates of all of the Patents-in-Suit.

54. One means of promoting payment security is "tokenization," an approach that substitutes sensitive data like account numbers and other personally identifiable information with a non-sensitive equivalent that has no intrinsic or exploitable meaning or value.

55. EMV payment tokens are open-loop tokens provisioned by a token service provider ("TSP"). Like other tokens, EMV payment tokens are used to replace the actual payment credential (*e.g.*, primary account number "PAN") with another numeric value.

56. The U.S. Payments Forum (formerly the EMV Migration Forum) is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of and enhance opportunities for payment transactions. According to the U.S. Payments Forum, Samsung was "among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases."

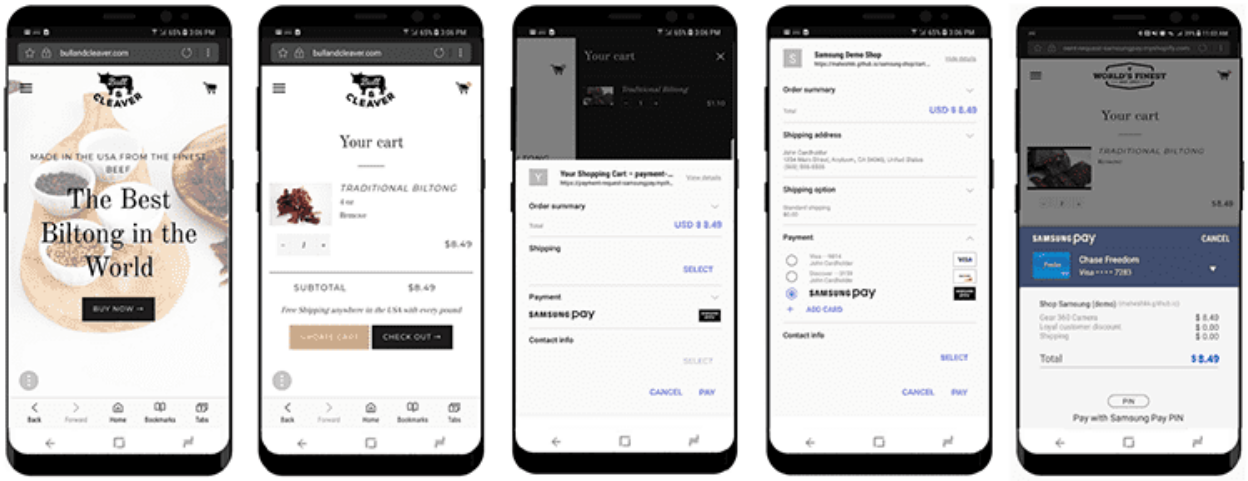
57. On information and belief, EMV payment tokens are issued to Samsung Pay equipped devices in exchange for a credit card number by a TSP such as Visa, Mastercard, American Express or Discover. On information and belief, device-specific payment tokens are stored by Samsung Pay-equipped devices.

58. The device-specific EMV payment tokens may be stored in three locations, one of them being a secure element / integrated circuit card ("ICC"). The first Samsung Pay-equipped devices, the Galaxy S6 and S6 Edge included a security cryptocontroller, *e.g.*, the Infineon SLE 97 ICC; on information and belief, subsequent devices equipped with Samsung Pay continued to use ICC elements. Secure elements like Infineon's SLE ICC are, according to the U.S. Payments Forum, "a dynamic environment to store data securely, process data securely and perform communication with external entities securely," that "will not allow unauthorized access."

59. Samsung Pay requests biometric verification before providing payment credentials to merchants. The location/type of the purchase determines how the request is initiated.

60. For example, integrating the Samsung Pay API into their websites permits a merchant to accept Samsung Pay. When implemented via integration of the Samsung Pay API,

"the user initiates checkout, selects Samsung Pay as the preferred payment method, authenticates with a fingerprint or PIN, and voila — payment complete." Samsung further describes that "[w]hen properly implemented, the API also supports editing the billing/shipping address in Samsung Pay and selecting a different enrolled card before approving the transaction with a fingerprint scan or entering a PIN." See **Exhibit 14** (Samsung's Web Payments Integration Guide). A standard W3C implementation of Samsung Pay to a standard PaymentRequest object is shown below:



61. Samsung Pay also works with merchant apps on a user's smartphone. On information and belief, merchant apps installed on a user's smartphone communicate with Samsung Pay through the Samsung Pay API. A general use case takes the following form, according to Samsung:

62. To initiate payment, a merchant app calls the startIn-AppPay function of the API, which "initiates payment request with Samsung Pay." When the merchant app calls startIn-AppPay, Samsung Pay responds by presenting the user "with a payment sheet, which includes card selection and shipping address confirmation." After being presented the payment sheet, "the user then authenticates the payment method, amount, and delivery address with a fingerprint."

63. Samsung Pay also operates using NFC and/or MST: "Combining NFC with Samsung's proprietary MST technologies, Samsung Pay provides consumers a way to pay almost anywhere you can swipe or tap a card at millions of merchant locations." *See* **Exhibit 15** (Samsung Pay Reaches One Year Anniversary in the United States, Samsung Newsroom (2016)). Samsung Pay equipped devices utilize the Android OS, as noted above. "Android 4.4 introduce[d] a new platform support for secure NFC-based transactions through Host Card Emulation (HCE), for

payments, loyalty programs, card access, transit passes, and other custom services." **Exhibit 16** (Android KitKat). When a user taps a phone to a payment terminal, "Android uses Application Identifiers (AIDs) as defined in ISO/IEC 7816-4 as the basis for routing transactions to the correct Android applications", such as the equipped Samsung Pay on Samsung's devices. When paying with Samsung Pay instore, "the app reads the transaction data and can use any local or network-based services to verify and then complete the transaction." *Id*. When opened in response to AID routing, Samsung Pay permits a user "to make a payment with [their] Favorite Cards, [by] swip[ing] up from the bottom of the screen. Then swip[ing] through and select[ing their] preferred card." *See* **Exhibit 17** (Make an in-store payment with Samsung Pay, Samsung Support). After selecting the card, the user "tap[s] PIN or IRIS . . . [or] simply place[s their] finger on [their] phone's fingerprint scanner". *Id.*.

64. Whether through AID routing, functions call between apps, or push notifications, regardless of where a user is shopping Samsung Pay equipped devices receive a request for biometric verification to authorize payment.

65. On Android devices like Samsung's devices, "the fingerprint sensor of [the] device is generally idle", but "in response to a call to authenticate . . . the fingerprint sensor listens for a touch". **Exhibit 18** (Android Open-Source Project: Fingerprint HIDL). After the user places their fingerprint on the sensor, a "vendor-specific library determines if there is a fingerprint match in the current set of enrolled fingerprint templates." *Id*.

66. Samsung Pay equipped devices wirelessly transmit EMV tokens to provide payment to merchants. When shopping online at a website, Samsung Pay equipped devices receive a push notification requesting authorization by the user, as detailed *supra*. "After user authenticates payment data is encrypted with partner's public key in user device, and will be sent

it to Samsung server" and made available to the merchant's website. **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12.

67. The series of requests and responses permitting the merchant to receive payment, as summarized in Figure 10.1 of the EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020), begins with the merchant submitting a Token Payment Request for transaction routing. **Exhibit 20**. The data included within the Token Payment Request, as detailed in Table 10.1 of **Exhibit 20** (EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020)), is required to contain the payment token.

68. During transaction routing within the payment network, the Token Payment Request is transformed to a Token Authorization Request, as detailed in Figure 10.1 of **Exhibit 20**. As detailed in Table 10.3 of **Exhibit 20**, a required field of the Token Authorization Request generated by routing the Token Payment Request through payment network is a payment token. Accordingly, the payment token sent in the Token Payment Request from the merchant continues to persist during the token authorization request process. EMV payment tokens uniquely identifying Samsung Pay equipped devices and are provided during card enrollment, and thus are an identified embodiment of device ID codes specifically mentioned in at least the 730, 905, and 989 Patents.

69. "The Token Authorisation request process continues until De-Tokenisation has been completed." **Exhibit 20**, page 86. De-Tokenisation is performed by the token service provider. Visa, MasterCard, American Express and Discover each take on the role as TSPs. **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers). "Token Service Providers are responsible for a number of discrete

functions which may include, but are not limited to: Maintenance and operation of a Token Vault . . . [and] De-Tokenisation". **Exhibit 20** (EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020)), page 19.

70. Maintaining the token vault and providing de-tokenisation, token service providers keep a list of device ID codes uniquely identifying legitimate integrated devices. The token vault maintained by Visa, MasterCard, and other token service providers is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data". Maintaining the mapping between payment tokens and underlying primary account numbers, the token vault represents a list of legitimate tokens. EMV payment tokens, as detailed above, are values uniquely identifying Samsung Pay-equipped devices provided during card enrollment, and thus are an identified embodiment of device ID codes. As tokens are embodiments of device ID codes, the listing of legitimate payment tokens maintained by token service providers as part of the token vault is an identified embodiment of a list of device ID codes uniquely identifying legitimate integrated devices. TSPs are therefore one embodiment of a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices.

71. Opening the token vault to perform de-tokenisation occurs in response to receiving the token authorization request containing the payment token. De-Tokenisation is "the process of converting a Payment Token and Token Expiry Date to its underlying PAN and PAN Expiry Date based on the Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date stored in the Token Vault." **Exhibit 20** at 6. "The Payment Token SHALL be de-tokenised to the underlying PAN in the incoming Token Authorisation prior to sending the PAN Authorisation to the Card Issuer." *Id.*, at 91. Detokenizing in response to an incoming token

authorization requests requires the token service provider be sent the token authorization. As noted above, the token authorization sent to the TSP contains the payment token wirelessly sent from a Samsung Pay-equipped smartphone after successful biometric authentication. Authenticating a user via biometrics, as noted above, entails a vendor-specific library on the Samsung Pay-equipped devices comparing scan data from a sensor to biometric data to determine whether the scan data matches the biometric data.

72. When providing payment for in-app purchases, Samsung Pay equipped devices wirelessly transmit EMV tokens to merchants as payment. Specifically, "Encrypted payment information is passed from the Samsung Pay to the PG [(Payment Gateway)] through the merchant app". **Exhibit 21** (Samsung Pay Developers Onboarding and Project Integration Guide: In-App Payments for Merchants, Doc Rev 3.1-US (2017)), page 17.

73. In addition to providing payment information via virtual terminals, Samsung Pay equipped devices "combin[e] NFC with Samsung's proprietary MST technologies [to provide] consumers a way to pay almost anywhere you can swipe or tap a card at millions of merchant locations." Tapping a credit card is an example of contactless payment. "In a contactless payment transaction, the consumer holds the contactless card, device, or mobile phone in close proximity (less than 2-4 inches) to the terminal and the payment account information is communicated wirelessly (via radio frequency [RF]) or NFC." **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 39. By utilizing NFC, Samsung Pay-equipped devices can wirelessly transmit payment information to in-store terminals.

74. After the purchase has been authorized, Samsung Pay equipped devices "receive a push notification with details of [the] transaction after each purchase." **Exhibit 23** (View recent transactions in Samsung Pay). As the purchase can only be made after the primary account number

mapped to the token was released from the token vault and placed in an authorization request sent to the card issuer, the push notification received indicates allowed access to the file containing the account number. As shown in Figures 6, 7 and 11 of **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), this confirmation of access is either sent directly from the token service provider or indirectly from the token service provider as one of series messages flowing back to the Samsung Pay equipped smartphone.

75. Samsung Pay functionality is not limited to Samsung smartphone and tablet devices. Samsung's Galaxy Watch series also integrates with Samsung Pay. Samsung advertises that "you can use Samsung Pay on your watch!" An image that appears on Samsung's support page titled "Setting up your Samsung smart watch with or without your phone" is reproduced below:

76. The same support page describes that "[t]o access all its fun and useful features, you'll want to connect your smart watch to your phone using the Galaxy Wearable app.." **Exhibit 24**. As such, a Samsung smartphone or tablet with the Samsung Galaxy Wearable app (Wear

App) installed may act a personal digital key. Samsung smartphones and tablets communicate wirelessly, via an integrated receiver-decoder circuit enabling communication via Bluetooth, for example, with the Samsung Galaxy Watch, which also contains a receiver-decoder circuit external to the phone or tablet.

77. Samsung smartphone and tablets utilize a system on a chip (SoC) such as, in the case of its latest Galaxy S21 model, the Qualcomm Snapdragon 888 which provides several wireless interfaces including 5G, LTE, Bluetooth, and Wi-Fi. When communicating over a Bluetooth wireless connection, a proximity zone between the two devices is inherent, as the Bluetooth range may be approximately 30 feet.

78. The SoC interfaces with the various system components including the secure element, which is utilized to store, *inter alia*, secure biometric information for authenticating a user. The SoC must, like other system components, also interface with the battery of the smartphone or tablet.

79. On information and belief, Samsung's execution environment for Samsung Pay on its Galaxy Watch series includes an embedded secure element ("eSE"). Samsung has indicated such to EMVCo, as per the EMVCo Letter of Approval for the Galaxy Watch Active 2. eSE provides embedded, secure storage to "keep mobiles safe" by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." **Exhibit 25** (Samsung Security Solutions, Embedded security keeps mobiles safe).

80. The personal digital key component of Samsung's devices enable, *inter alia*, Samsung Pay.

81. Proxense has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit. On information and belief, any prior assignees and licensees have also complied with the marking provisions of 35 U.S.C. § 287.

CLAIM 1
(Infringement of the 730 Patent)

82. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

83. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 730 Patent.

84. Samsung infringes at least claims 1, 2, 5, 6, 8, and 9 of the 730 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

85. For example, Samsung directly infringes at least claim 1 and 5 of the 730 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States the software application Samsung Pay and products including Samsung Pay (*see* Appendix A). That software performs/executes, and those products provide, a method for verifying a user during authentication of the device.

86. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint and/or iris profile of a user, and codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value, in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered. Samsung devices utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example,

Samsung devices may utilize Fingerprint Hardware Interface Definition Language (HIDL) provided by Android which limits access to, and the ability to alter, biometric data.

87. Samsung devices with Samsung Pay safeguard financial information, *e.g.*, credit card information, with EMV payment tokens as described *supra*. Indeed, Samsung was among the first to implement EMV payment tokens in digital wallets that hold credentials. On information and belief, the EMV payment tokens utilized by Samsung Pay uniquely identify the Samsung device. On further information and belief, the payment tokens are stored in a secure element that is tamper proof, *e.g.*, the Infineon SLE 97 ICC chip in the Galaxy S6 and S6 Edge. Secure elements are recognized as "a dynamic environment to store data securely, process data securely and perform communication with external entities securely," that "will not allow unauthorized access."

88. Samsung devices with Samsung Pay also contain a secret decryption value, also called a "private key," which is used for, *inter alia*, decrypting, as specified in Android's keymaster functions, which provide hard-backed cryptography for secure key storage in a secure environment, such as the TEE, described *supra*. The secret decryption value, like the biometric data of the user and plurality of codes and other data values comprising a device idea, is tamper-proof as a result of being securely stored by the Samsung devices.

89. As described *supra*, Samsung devices with Samsung Pay may utilize biometric data, such as fingerprint and/or retina scan data from a biometric scan, and verify (*e.g.*, authenticate) biometric data of a user. The location of a purchase may determine how the request for verification is received (*e.g.*, a push notification received from a merchant's website, an API call from a merchant apps installed on the device, or direct prompt for Samsung Pay when using NFC (or MST) in stores). When a Samsung device utilizes and verifies fingerprint biometric data,

for example, scan data is compared with the fingerprint data on the device to determine whether there is a match.

90. After receiving the determination that the scan data matches the biometric data, Samsung devices with Samsung Pay wirelessly send one or modes codes, including device ID codes, regardless of where the user is shopping. For example, Samsung devices wirelessly transmit EMV payment tokens. EMV payment tokens, as detailed *supra*, are values uniquely identifying Samsung Pay preloaded smartphones provided during card enrollment, and thus are an identified embodiment of device ID codes. The payment tokens may be authenticated by an agent, *e.g.*, a token service provider.

91. Samsung devices with Samsung Pay are also responsive to an access message from agents that are a third-party trusted authority, e.g., token service providers which are responsible for, *inter alia*, de-tokenization. These providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token, which includes one or more codes from a plurality of codes and other data values including a device ID device, wirelessly transmitted by a Samsung device to the tokens stored in its repository for authenticated.

92. Samsung devices with Samsung Pay are further responsive to authentication by the agent, *e.g.*, token service providers, of the one or more codes and the other data values. For example, Samsung devices with Samsung Pay "receive a push notification with details of [the] transaction after each purchase," *e.g.*, an access message. The push notification from the agent indicates that the user has been allowed access to an application, for example, an ATM machine, computer software, a web site and/or a file, *e.g.* which permits payment to occur.

93. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 730 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

94. Samsung also contributes to infringement by others of one or more claims of the 730 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 730 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

95. Samsung received constructive notice of the 730 Patent at least as early as July 2017 and actual notice of the 730 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 730 Patent.

96. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 730 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

97. Upon information and belief, Samsung will continue to infringe the 730 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 730 Patent by Samsung.

CLAIM 2
(Infringement of 905 Patent)

98. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

99. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 905 Patent.

100. Samsung infringes at least claims 1, 4, 5, 7, 9, 10, and 12 of the 905 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

101. For example, Samsung directly infringes at least claim 1 of the 905 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay and products that are with Samsung Pay (see Appendix A). That software performs/executes, and those products provide, the method of claim 1, for example.

102. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint or retina data, and an ID code, *e.g.*, a device-specific code that uniquely identifies a specific Samsung device. Samsung devices further utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example, Samsung devices utilize Fingerprint Hardware Interface Definition Language (HIDL) provided by Android which limits access to, and the ability to alter, biometric data.

103. As for the device specific code, on information and belief, payment tokens are unique for each device, as required by EMV. "Samsung [was] among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases." **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12. "EMV payment tokens are open-loop tokens provisioned by a TSP and, like other tokens, are used to replace the actual payment credential (e.g., PAN) with another numeric value." *Id.*, at 8. Payment tokens, accordingly, are issued ("provisioned") to Samsung Pay preload smartphones in

exchange for a credit card number by a token service provider (TSP), such as Visa, MasterCard, Discover, and American Express. *Id*., at 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers).

104. As described *supra*, Samsung devices with Samsung Pay may receive biometric data, such as fingerprint and iris-scanning, to verify a user. The location of a purchase may determine how the request for verification is received (*e.g*., a push notification received from a merchant's website, an API call from a merchant apps installed on the device, or direct prompt for Samsung Pay when using NFC (or MST) in stores).

105. For example, on a Samsung Pay equipped website, a "user can select 'Samsung pay' option to pay, and then payment requesting push message will [] arrive[] to [a] user's device and the payment can be confirmed by user authentication." **Exhibit 26** (Samsung Pay Web checkout Integration guide, Document version 1.4 (2018)), page 7. When the user clicks on the push notification received on their Samsung Pay preload smartphone, a "Payment Sheet is opened [and] User authentication is performed" giving the user the option to "pay with fingerprint". *Id*., at 6. Receiving a push notification prompting the user to authenticate by paying with their fingerprint, Samsung Pay preloaded smartphones therefore receive a request for biometric verification. Furthermore, Samsung devices with Samsung Pay receive scan data from a biometric scan carried out on a biometric sensor in response to receiving a request for biometric verification of a user.

106. When a Samsung device utilizes and authenticates fingerprint biometric data, for example, scan data from the fingerprint sensor of the device is compared with the existing fingerprint data on the device to determine whether there is a match.

107. After authenticating a user, Samsung devices with Samsung Pay wirelessly transmit one or modes codes, including device specific ID code, regardless of where the user is shopping. For example, Samsung devices wirelessly transmit EMV payment tokens which contain codes uniquely identifying the Samsung Pay device provided during card enrollment.

108. Samsung devices with Samsung Pay are also responsive to an access message from agents that are a third-party trusted authority, *e.g.*, token service providers which are responsible for, *inter alia*, de-tokenization. These providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token wirelessly transmitted by the Samsung device to the tokens stored in its repository, which include previously registered ID codes.

109. After an ID code has been authenticated by a third-party trusted authority, Samsung devices with Samsung Pay "receive a push notification with details of [the] transaction after each purchase," *e.g.*, an access message. At this point, whereby the third-party trusted authority has confirmed that it successfully authenticated the token (*e.g.*, including the ID code), the user is allowed to complete a financial transaction.

110. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 905 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

111. Samsung also contributes to infringement by others of one or more claims of the 905 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly

infringe the 905 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

112. Samsung received actual and constructive notice of the 905 Patent on or around July 2017. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 905 Patent.

113. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 905 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

114. Upon information and belief, Defendant will continue to infringe the 905 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 905 Patent by Defendant.

CLAIM 3
(Infringement of 989 Patent)

115. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

116. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 989 Patent.

117. Samsung infringes at least claims 1-6 of the 989 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

118. For example, Samsung directly infringes at least claim 1 of the 989 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay and products that are with

Samsung Pay (see Appendix A). That software performs/executes, and those products provide, a method for verifying a user during authentication of a device.

119. As described *supra*, Samsung devices are approved by EMVCo. "Samsung [was] among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases." **Exhibit 19**(EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12. "EMV payment tokens are open-loop tokens provisioned by a TSP and, like other tokens, are used to replace the actual payment credential (*e.g.*, PAN) with another numeric value." *Id*., p. 8. "As a part of provisioning an individual account or PAN, the token service generates a token, maps it to the PAN, and sends it to the token requestor." *Id.*, at page 16. "[T]he TSP acts as a trusted service manager (TSM), delivering the token over the air or over an Internet connection to a device," *e.g.*, Samsung devices with Samsung Pay. *Id*., p. 12. "As a part of provisioning an individual account or PAN, the token service generates a token, maps it to the PAN, and sends it to the token requestor." *Id.*, at page 16. This token, received by the Samsung devices, therefore contains an ID code that uniquely identifies the smartphone among a plurality of smartphones.

120. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint or iris profile of a user, and an ID code, *e.g.*, a device-specific code that uniquely identifies a specific Samsung device. Samsung devices further utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example, Samsung devices utilize Fingerprint Hardware Interface Definition Language (HIDL) which limits access to, and the ability to alter, biometric data.

121. As for the device specific code, on information and belief, payment tokens are unique for each device, as required by EMV. Payment tokens are issued ("provisioned") to

Samsung devices with Samsung Pay in exchange for a credit card number by a token service provider (TSP), such as Visa, MasterCard, Discover, and American Express. *Id*., at 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers).

122. As described *supra*, Samsung devices with Samsung Pay may receive biometric data, such as fingerprint and retina data, and authenticate such biometric data. The location of the purchase determines the type of verification carried out (*e.g*., a merchant's website, merchant apps installed on the device, or use of NFC (or MST) that provides a "way to pay almost anywhere you can swipe or tap a card at millions of merchant locations."

123. For example, on a Samsung Pay equipped website, a "user can select 'Samsung pay' option to pay, and then payment requesting push message will [] arrive[] to [a] user's device and the payment can be confirmed by user authentication." **Exhibit 26**, page 7. When the user clicks on the push notification received on their Samsung Pay preload smartphone, a "Payment Sheet is opened [and] User authentication is performed" giving the user the option to "pay with fingerprint". *Id*., at 6. As part of the authentication, Samsung devices with Samsung Pay receive scan data from a biometric scan using the smartphone.

124. Where a Samsung device utilizes and authenticates fingerprint biometric data, for example, scan data is compared with the fingerprint data on the device to determine whether there is a match.

125. After authenticating a user (*e.g*., making a determination that the scan data matches the biometric data), a Samsung device with Samsung Pay wirelessly sends one or modes codes, including device specific ID code, regardless of where the user is shopping, to a third-party trusted authority, *e.g*., token service providers. For example, Samsung devices wirelessly transmit EMV

payment tokens which contain codes uniquely identifying the Samsung Pay device provided during card enrollment.

126. Token service providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token wirelessly transmitted by the Samsung device to the tokens stored in its repository, which include previously registered ID codes.

127. In response to a purchase having been authorized (e.g., after successful comparison of the token sent by the Samsung device to the token(s) stored in the repository) by the provider, the transaction is completed and the Samsung device "receive[s] a push notification with details of [the] transaction after each purchase." The transaction includes either access to an ATM machine or a financial account (e.g., a credit card).

128. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 989 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

129. Samsung also contributes to infringement by others of one or more claims of the 989 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 989 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

130. Samsung received constructive notice of the 730 Patent at least as early as July 2017 and actual notice of the 989 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement,

with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 989 Patent.

131. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 989 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

132. Upon information and belief, Defendant will continue to infringe the 989 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 989 Patent by Defendant.

CLAIM 4
(Infringement of 188 Patent)

133. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

134. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 188 Patent.

135. Samsung infringes at least claims 1, 3-10, and 13-16 of the 188 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

136. For example, Samsung directly infringes at least claims 1 and 10 of the 188 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay, the Samsung Galaxy Wearable App and/or products that are with Samsung Pay (see Appendix A). Samsung Pay and/or the Samsung Galaxy Wearable App performs/executes the method of claim 10 and those products provide the hybrid device of claim 1, for example.

137. As described *supra*, Samsung devices with the Samsung Galaxy Wearable app enables applications on a paired Galaxy Watch to access memory on the smartphone or tablet, which stores local, secured biometric information.

138. The key utilized by the Wear App to control access to the memory of the Android smartphone by a paired Galaxy Watch may take on various forms. The key may be a cryptographic key such that an "encryption engine 254 encrypts/decrypts data 228 flowing to/from the service block 112 based on the access key 118 (or some other key generated based on the access key, for example a session key)". 188 Patent, Col. 6, ll. 33-37. In lieu of cryptology, the key may uniquely identify the paired Galaxy Watch. In such instances, the key may be "a PDK ID 212 [] used as an identifying feature of a PDK 102 and distinguish[ing] between PDKs 102 in private or Central registry entries". *Id*., Col. 5, ll. 66 to Col. 6, ll. 2. Besides a unique identifier or crypto-key, the key used by the Wear App to control memory access by a paired Galaxy Watch may be a "basic authentication function that allows the PDK and sensor to verify each other. In this scenario, once the sensor and PDK finish their verification the application is signaled". *Id*., Col. 9, ll. 28-31 ("[T]he RDC 304a represents and includes the functionality described above as being provided by the sensor 108." Id, Col. 13, ll. 58-60.).

139. Whether a crypto-key, unique identifier, or basic authentication, the Wear App functions as a controller by utilizing access keys to control access to the smartphone's memory. Pairing a Galaxy Watch to an Android 6.0 and higher smartphone via Bluetooth, the Wear App acting as a controller has access to each of these types of keys. "When a device is paired, the basic information about the device – such as the device's name, class and MAC address – is saved". **Exhibit 27** (Bluetooth Overview, Android Developers). Pairing a Galaxy Watch with an Android smartphone, accordingly, provides various identification keys usable by the Wear App to control

access to memory. Additionally, "to be *paired* means that two devices … have a shared link-key that can be used for authentication, and are capable of establishing an encrypted connection". *Id*. By pairing a Galaxy Watch with the Samsung device, the Wear App also gains access to authentication keys and crypto keys, which may be used to control access to the phone's memory. Samsung devices with the Samsung Galaxy Wearable app therefore comprise a personal digital key.

140. Samsung devices, including those with the Samsung Galaxy Wearable app, store local, secured biometric information as per Android's implementation guidelines which require tamper-proof "raw fingerprint data or derivatives (for example, templates) [that] must never be accessible from outside the sensor driver or TEE" (trusted execution environment) and "fingerprint acquisition, enrollment, and recognition must occur inside the TEE". Exhibit R (Android Open-Source Project: Fingerprint HIDL). Per these guidelines, biometric information, *e.g.*, fingerprint data never leaves the TEE. Furthermore, Android's TEE, called Trusty, "uses ARM's Trustzone™ to virtualize the main processor and create a secure trusted exaction environment" isolated from the rest of the system. **Exhibit 28** (Android Open-Source Project: Trusty TEE). Accordingly, biometric information, *e.g.*, fingerprint data, which never leaves the TEE, also never leaves the Trustzone housing, Trusty.

141. The integrated personal digital key of the Samsung devices with the Samsung Galaxy Wearable app is also capable of communicating wireless with an external receiver-decoder circuit. For example, using Bluetooth, which is provided through SoCs integrated into Samsung devices, e.g. Qualcomm's Snapdragon, the personal digital key may communicate with a Samsung Galaxy Watch. As detailed by Samsung, "Install the Galaxy Wearable application on your mobile device, then pair your wearable devices via Bluetooth to enjoy all of its features." Galaxy

Wearable, App on Google Play. Pairing a device and a watch with the Samsung Galaxy Wearable app via Bluetooth further requires the paired Samsung Galaxy Watch to have an external receiver decoder circuit to the smartphone. A Samsung device with the Wear App, therefore, contains an "integrated personal digital key (PDK) … capable of communicating wirelessly with an external receiver-decoder circuit (RDC)".

142. As described above, the Samsung devices include a SoC with a receiver decoder circuit which provides, inter alia, Bluetooth capability. The receiver decoder circuit communicates wireless (*e.g.*, via Bluetooth) with an external personal digital key—e.g., a Samsung Galaxy Watch. With their own counterpart to the Wear App to enable pairing over a Bluetooth, as well as an embedded secure element (eSE) storing payment information, Samsung Galaxy Watches constitute personal digital keys.

143. In addition to a Bluetooth transceiver communicating with an RDC, Samsung Galaxy Smart watches have an eSE storing information particular to a user. One feature enabled by pairing a Samsung Galaxy Watch to an Android 6.0 and higher smartphone is the ability to use Samsung Pay on the paired Galaxy Watch. Adding a credit card to Samsung Pay on a Galaxy watch requires, "[o]n your phone, open[ing] the Galaxy Wearable app… then tap[ping] Add credit or debit card." **Exhibit 29** (Add a payment card to Samsung Pay). The user may then "take a photo of the card number or manually enter them". Id. Regardless of how entered, the card information must get from the phone to the Galaxy Watch, most likely as a EMV Payment Token received on the phone in response to a request by Samsung Pay to a Token Service Provider (TSP), and then be stored on the Galaxy Watch.

144. Samsung identifies the execution environment of Samsung Pay on, for example, the Samsung Galaxy Watch Active 2 as including an eSE (embedded secure element). Exhibit 13,

EMVCo Letter of Approval – EMV Contactless Level 1 Mobile Product, Approval No. MTA_LOA_SAEL_02082, page 2 (identifying the "execution environment" as including an "eSE"). Samsung describes that its eSE provides secure storage by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." Exhibit 25 (Embedded security keeps mobiles safe). Credit card information (EMV Payment Token) received from the Samsung smartphone or tablet is therefore stored in the eSE on the watch. A Galaxy Watch paired to the PDK provided on Samsung smartphone or tablet by the Wear App, therefore contains memory storing information particular to a user.

145. The integrated receiver decoder circuit of the smartphone or tablet, e.g. the SoC, is coupled to the personal digital key by a first signal line. As described *supra*, a Samsung device with the Samsung Galaxy Wearable app requires "storage" permission "used to transmit and receive stored files" with a Samsung Galaxy Watch and therefore a first signal line is used to transmit files from storage to the SoC. The integrated receiver decoder circuit is also coupled to, *inter alia*, the device's battery.

146. Ultimately, the personal digital key of a Samsung device with the Samsung Galaxy Wearable app may enable, inter alia, Samsung Pay. "Instal[ing] the Galaxy Wearable application on your mobile device, then pair[ing] your wearable devices via Bluetooth [allows you] to enjoy all of its features." Galaxy Wearable, App on Google Play. "Before you can use Samsung Pay on your watch, you need to connect your watch to your phone". Exhibit 29 (Add a payment card to Samsung Pay). "After initial setup, Samsung Pay on Galaxy Watch can make at least five transactions without reconnecting to a network… via Bluetooth pairing with compatible smartphone." Exhibit 30 (Samsung Galaxy Watch – Our Newest Smartwatch, Samsung US).

147. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 188 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

148. Samsung also contributes to infringement by others of one or more claims of the 188 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 188 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

149. Samsung received actual and constructive notice of the 188 Patent on or around July 2017. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 188 Patent.

150. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 188 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

151. Upon information and belief, Defendant will continue to infringe the 188 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 188 Patent by Defendant.

CLAIM 5
(Infringement of 700 Patent)

152. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

153. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 700 Patent.

154. Samsung infringes at least claims 1, 3, 5-9, 11, 15-17 and 19 of the 700 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

155. For example, Samsung directly infringes at least claims 1 and 11 of the 188 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay, the Samsung Galaxy Wearable App and/or products that are with Samsung Pay (see Appendix A). Samsung Pay and/or the Samsung Galaxy Wearable App performs/executes the method of claim 11 and those products provide the hybrid device of claim 1, for example.

156. As described *supra*, Samsung devices with the Samsung Galaxy Wearable app enables applications on a paired Galaxy Watch to access memory on the smartphone or tablet, which stores local, secured financial information.

157. Whether a crypto-key, unique identifier, or basic authentication, the Wear App functions as a controller by utilizing access secured financial information (*e.g.*, keys) to control access to the smartphone's memory. Pairing a Galaxy Watch to an Android 6.0 and higher smartphone via Bluetooth, the Wear App acting as a controller has access to each of these types of keys. "When a device is paired, the basic information about the device – such as the device's name, class and MAC address – is saved". **Exhibit 27** (Bluetooth Overview, Android Developers). Pairing a Galaxy Watch with an Android smartphone, accordingly, provides various identification keys usable by the Wear App to control access to memory. Additionally, "to be *paired* means that two devices … have a shared link-key that can be used for authentication, and are capable of establishing an encrypted connection". *Id.* By pairing a Galaxy Watch with the Samsung device,

the Wear App also gains access to authentication keys and crypto keys, which may be used to control access to the phone's memory. Samsung devices with the Samsung Galaxy Wearable app therefore comprise a personal digital key.

158. The integrated personal digital key of the Samsung devices with the Samsung Galaxy Wearable app is also capable of communicating wireless with an external receiver-decoder circuit. For example, using Bluetooth, which is provided through SoCs integrated into Samsung devices, *e.g*. Qualcomm's Snapdragon, the personal digital key may communicate with a Samsung Galaxy Watch. As detailed by Samsung, "Install the Galaxy Wearable application on your mobile device, then pair your wearable devices via Bluetooth to enjoy all of its features." Galaxy Wearable, App on Google Play. Pairing a device and a watch with the Samsung Galaxy Wearable app via Bluetooth further requires the paired Samsung Galaxy Watch to have an external receiver decoder circuit to the smartphone. A Samsung device with the Wear App, therefore, contains an "integrated personal digital key (PDK) … capable of communicating wirelessly with an external receiver-decoder circuit (RDC)".

159. As described above, the Samsung devices include a SoC with a receiver decoder circuit which provides, *inter alia*, Bluetooth capability. The receiver decoder circuit communicates wireless (*e.g.*, via Bluetooth) with an external personal digital key—*e.g*., a Samsung Galaxy Watch. With their own counterpart to the Wear App to enable pairing over a Bluetooth, as well as an embedded secure element (eSE) storing payment information, Samsung Galaxy Watches constitute personal digital keys.

160. In addition to a Bluetooth transceiver communicating with an RDC, Samsung Galaxy Smart watches have an eSE storing information particular to a user. One feature enabled by pairing a Samsung Galaxy Watch to an Android 6.0 and higher smartphone is the ability to use

Samsung Pay on the paired Galaxy Watch. Adding a credit card to Samsung Pay on a Galaxy watch requires, "[o]n your phone, open[ing] the Galaxy Wearable app… then tap[ping] Add credit or debit card." **Exhibit 29** (Add a payment card to Samsung Pay). The user may then "take a photo of the card number or manually enter them". *Id*. Regardless of how entered, the card information must get from the phone to the Galaxy Watch, most likely as a EMV Payment Token received on the phone in response to a request by Samsung Pay to a Token Service Provider (TSP), and then be stored on the Galaxy Watch.

161. Samsung identifies the execution environment of Samsung Pay on, for example, the Samsung Galaxy Watch Active 2 as including an eSE (embedded secure element). Exhibit 13, EMVCo Letter of Approval – EMV Contactless Level 1 Mobile Product, Approval No. MTA_LOA_SAEL_02082, page 2 (identifying the "execution environment" as including an "eSE"). Samsung describes that its eSE provides secure storage by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." Embedded security keeps mobiles safe, http://www.samsung.com/semiconductor/security/ese/. Credit card information (EMV Payment Token) received from the Samsung smartphone or tablet is therefore stored in the eSE on the watch. A Galaxy Watch paired to the PDK provided on Samsung smartphone or tablet by the Wear App, therefore contains memory storing information particular to a user.

162. The integrated receiver decoder circuit of the smartphone or tablet, e.g. the SoC, is coupled to the personal digital key by a first signal line. As described *supra*, a Samsung device with the Samsung Galaxy Wearable app requires "storage" permission "used to transmit and receive stored files" with a Samsung Galaxy Watch and therefore a first signal line is used to

transmit files from storage to the SoC. The integrated receiver decoder circuit is also coupled to, *inter alia*, the device's battery.

163. Ultimately, the personal digital key of a Samsung device with the Samsung Galaxy Wearable app may enable, *inter alia*, Samsung Pay. "Instal[ing] the Galaxy Wearable application on your mobile device, then pair[ing] your wearable devices via Bluetooth [allows you] to enjoy all of its features." Galaxy Wearable, App on Google Play. "Before you can use Samsung Pay on your watch, you need to connect your watch to your phone". Exhibit 29 (Add a payment card to Samsung Pay). "After initial setup, Samsung Pay on Galaxy Watch can make at least five transactions without reconnecting to a network… via Bluetooth pairing with compatible smartphone." Exhibit 30 (Samsung Galaxy Watch – Our Newest Smartwatch, Samsung US).

164. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 700 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

165. Samsung also contributes to infringement by others of one or more claims of the 700 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 188 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

166. Samsung received constructive notice of the 700 Patent at least as early as July 2017 and actual notice of the 700 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 700 Patent.

167. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 700 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

168. Upon information and belief, Defendant will continue to infringe the 700 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 188 Patent by Defendant.

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a jury trial of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief against Defendants as follows:

a. Entry of judgment declaring that Defendants infringe one or more claims of each of the Patents-in-Suit;

b. Entry of judgment declaring that Defendants' infringement of the Patents-in-Suit is willful;

c. An order awarding damages sufficient to compensate Plaintiff for Defendants' infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, including supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

d. Enhanced damages pursuant to 35 U.S.C. § 284;

e. Entry of judgment declaring that this case is exceptional and awarding Plaintiff its costs and reasonable attorney fees pursuant to 35 U.S.C. § 285;

f. An accounting for acts of infringement;

g. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

h. Such other and further relief as the Court deems just and proper.

Dated: March 5, 2021

Respectfully submitted,

/s/ Erick S. Robinson

David L. Hecht (PHV to be submitted) (**lead counsel**)
Maxim Price (PHV to be submitted)
Conor B. McDonough (PHV to be submitted)
Yi Wen Wu (PHV to be submitted)
James Zak (PHV to be submitted)
dhecht@hechtpartners.com
mprice@hechtpartners.com
cmcdonough@hechtpartners.com
wwu@hechtpartners.com
jzak@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, NY 10017
P: (212) 851-6821
dhecht@hechtpartners.com

-and-

Erick S. Robinson
Texas Bar No. 24039142
erobinson@porterhedges.com
PORTER HEDGES LLP
1000 Main Street, 36th Floor
Houston, Texas 77002
P (713) 226-6615
F: (713) 226-6215

ATTORNEYS FOR PLAINTIFF
Proxense, LLC